1955

~~TOP SECRET "B"~~ TICOM/I-118

JOINT REPORTS BY REG. RAT. DR. HUETTENHAIN AND SDF.DR. FRICKE, WRITTEN AT OSDIO ON OR ABOUT 28th AUTUST, 1945.

Subject matters contained in the attached translations are as follows:-

a. Cryptographic course at OKW/Chi.

b. Austrian Cryptographic Dept.

c. Speech De-scrambling at LUDWIGSFELDE.

d. Mustang speech encyphering apparatus.

e. Cypher Machine M 40.

f. Solution of Japanese Diplomatic Messages.

g. The solution of Polish Attaché Messages.

Ticom Copy No. 23

24th Sept. 1945 No. of pages. 9

DISTRIBUTION

British

1. D.D.3
2. H.C.G.
3. D.D. (N.S.)
4. D.D. (M.W.)
5. D.D. (A.S.)
6.)
7.) C.C.R. (2)
8. Lt. Col. Leathem
9. Cdr. Tandy
10. Major Morgan

U.S.

11.)
12.) Op-20-G (2) (via Lt.Cdr.Manson)
13. G-2 (via Lt.Col.Hilles)
14.)
15.)
16.) A.S.A. (3) (via Major Seaman)
17. Director, S.I.D. USFET (via Lt.Col. Johnson)
18. Col. Lewis Powell, USSTAF.

Ticom

19. Chairman
20.) S.A.C. (2)
21.)
22. Cdr. Bacon
23. Lt. Col. Johnson
24. Major Seaman
25. Lt. Cdr. Manson
26. Major Cowan
27. Lt. Fehl
28.)
29.)
30.)
31.) Ticom Files (4)

Additional

32. S.A.C. for Capt. Ginsburg
33. Mr. Twinn

Do NOT Destroy Return to the NSA Technical Library when no longer needed
S-4750 TICOM No. 9

Approved for Release by NSA on 07-25-2017, FOIA Case # {66109}

Doc ID: 6587328

CRYPTANALYTIC COURSES AT OKW/CHI

Since about 1930, cryptanalytic courses have been held at Chi for 6-monthly periods over the Winter. Each new member of the staff had to take part in two consecutive courses. In the first 6-monthly Winter period, the fundamental systems of substitution methods were dealt with, that is to say substitutions (simple, multiple, variable unit ((wechselstelliger)), syllabic), substitution systems (periodic and aperiodic), bigram substitution ((Paaraesaren)) and code-books.

In the second 6-monthly Winter period, the basic transposition systems were first dealt with (local transposition ((umstellung)), simple transposition, transposition with diagonals, comb transposition and stencils) and then the principal recyphering methods (combinations of basic systems, further substitution, subtractors and dummy recypherments, ((Blender ueberschluesselung))).

The different encyphered texts were worked on alongside practice-examples based on German P/L texts.

Two periods of instruction, each lasting two hours were held each week, so that in one half-year there would be about 50 two-hour periods. The number of participants varied considerably from one 6-monthly period to another. Some courses were attended by 3, others by as many as 12 persons and more. In the first years, Min.Rat.FENNER directed all the courses personally; later, FENNER and Dr. WENDLAND divided this work between them. During the war these beginners' courses were held by Dr. WENDLAND and Dr. HUETTENHAIN.

Only the newly engaged staff of the sections dealing with the various countries took part in these courses. Members of the cryptanalytic section, as soon as they joined, were immediately instructed at Chi for 2 to 4 months of their service period in fundamental and recyphering systems, so that after that period had elapsed they would be in a position to tackle unsolved problems on their own.

In the Summer of 1943, a course of advanced study was instituted for the first time. 8 capable decypherers, who had shown some cryptanalytic ability, were detached from the sections dealing with the various countries and joined this course. Three 2-hour periods took place each week, in Summer and Winter. The duration of the course was not fixed at the outset. As a result of the general situation, no more instruction was given after November 1944. Dr. HUETTENHAIN was in charge of the course.

The breaking of recypherments was worked at exclusively. At first, the mathematical bases ((of cryptanalysis)) were worked through, for example, permutations, the theory of probabilities, elementary statistics. Then the relavant cryptanalytic problems were treated; solving of compromised text , investigation of indicator-groups, subtractor problems of general and particular application, special solving of double-transpositions etc. Machine cyphers were also to have been dealt with in this course. To conclude these theoretical studies, problems were examined

/which

Doc ID: 6587328

which had actually occurred and then, when possible, the study of these was carried still further. Those taking part in the course were familarised with the working of HOLLERITH machines and mechanical aids to cryptanalysis. A study was also made of the methods of breaking our own cyphers discovered by the cypher security people. In brief, this course was intended as instruction in cryptanalysis as it stood at the time.

Translator: J.M.E.

(CSDIC)
28/8/45.

Crypto Office in Austria

Until the Anschluss there was a cryptographic office in Vienna which collaborated closely with the Chancellory Office of the Bund and decyphered diplomatic messages. The head of this office was Hofrat Dr. SEIFERT. The staff was small. Italy, Roumania, Greece, Jugoslavia, Bulgaria, Turkey, Poland and Czechoslovakia were the countries dealt with. This office has worked in close contact with "Chi" ((i.e. OKW/Chi)) for many years. We do not know, however, in detail what this collaboration amounted to.

During tension between the two countries, the collaboration between the two "Chi" offices was maintained. When the Anschluss was effected, General FELIGIEBEL and Min. Rat. FENNER brought the best personnel to Berlin. The following joined "Chi": Hofrat Dr. SEIFERT who was a Min. Rat. in Berlin, Dr. MAULER and Reg. Rat Dr. LOCKER. Herr BAILOVIC came to the Forschungsamt; he only stayed a short time with FA and was then taken over by the Army (In. 7) and for the last 4 months was ORR at Chi.

At Chi the above named were given the following tasks:-

Dr. SEIFERT was specialist on known codes and broke Polish, Turkist, Greek and Vatican basic books.

Dr. MAULER was deputy head of the Italian Section.

Dr. LOCKER was head of the Turkish Section.

ORR BAILOVIC worked on Balkan Codes and cyphers.

Translator. W.G.O.

/Speech

Doc ID: 6587328

Speech de-scrambling apparatus at LUDWIGSFELDE

There was an intercept apparatus at Ludwigsfelde by which "encyphered" conversations between London and Washington were picked up in deciphered form. The principle of the enciphering is unknown to us now. At any rate it was such a simple matter that when using a new key, this new key could be found in a few minutes. It was only necessary to turn a few knobs until the speech became intelligible again.

The equipment was constructed in accordance with information from Wa Pruef 7 and in such a way that it could still have been used if the key had been extended but preserving the basic principle. We do not know if there was a second apparatus at another station in Germany of this or similar type. No secret conversations were allowed on the London-Washington line. If the subscribers ignored this regulation they were told about it through a "speaker". If necessary, the conversation was cut off.

Translator: W.G.O.

MUSTANG Speech Encypherment

In the Spring of 1945, a speech encypherment apparatus, recovered intact from a MUSTANG fighter, was submitted by the G.A.F. to certain members of the 3 branches of the Armed Forces and OKW/Chi at ADLERSHORST near BERLIN. The decision was taken on that occasion to hand the set over to Wa Pruef 7, for more detailed examination. The intention was to discover the degree of security provided by the set, and, if possible, to construct a set which would enable us to listen in to the traffic.

The investigations into the security, which were conducted mainly by Dr. BUGGISCH and Dr. LOTZE, were inconclusive. Only the following points were established:

1) The TIGERSTEDT cypher principle is used; there are 9 subscribers (sprechkoepfe).

2) The number of possible key settings is so great that the systematic examination of all keys would probably not lead to a solution.

3) It is always possible to reconstruct the key-setting from an intercepted ((aufgenommenen)) oscillogram. It is doubtful, however, whether the solution can be reached in a short enough time for exploitation during the actual fighter operation concerned.

Translator: J.M.E.

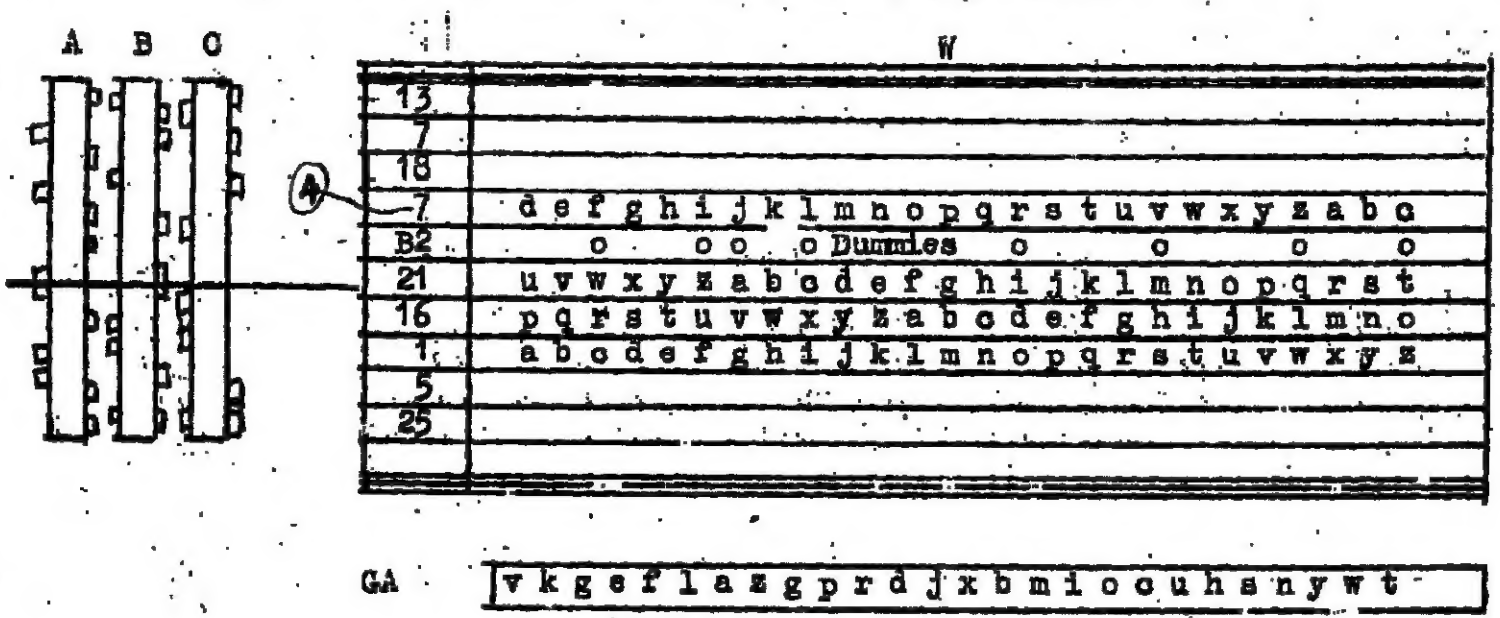
/Cypher

Doc ID: 6587328

Cypher Machine M 40

Cypher machine M 40 was designed and constructed by Ob. Insp. MENZER over the period 1937-1939. After the designs had been completed, Wa Pruef had 30 machines built by the firm of Wanderer in Chemnitz. However, as far as we know, they were never used. Exact information on all details cannot be given, as some points have slipped our memory. For this reason, all figures given in this report are to be accepted with reserve.

29 metal bars were fitted to the drum W (see diagram).



These bars were numbered 1 to 26 and B1, B2 and B3. On bars 1 to 26 the letters of the alphabet were cylically arranged, in alphabetical order. Bars B1 to B3, the so-called "dummy strips" ((Blenderstreifen)), bore small circles at 8 or 9 different points. All the metal bars but one were covered up by the machine lid. Under the window in the lid ((through which one of the bars marked with an alphabet appeared)) the cypher alphabet GA was inscribed. The clear letter was looked up on the metal bar which happened to be visible at the time, and substituted by the cypher letter occurring below it ((on the lid)). Decypherment was effected by the reverse process. The drum with the bars turned on its own axis and was made to move by the depression of a key. For each depression of the key the drum gave 1, 2, 3 or 4 kicks. The movement of the drum was controlled by the 3 pin-wheels A, B and C. These pin-wheels were fitted with variable pins and had periods of 23, 24 and 25. If none of the pins on the pin-wheels was in the "effective" position, then the drum gave one kick; if one of the pins on any of the wheels was "effective", the drum gave two kicks; for two "effective" pins, three kicks; for three "effective" pins four kicks. If a dummy bar appeared in the window on the lid, a letter coming below one of the circles on the dummy bar was inserted in the text as a dummy. The letter to be encyphered was then encyphered after another depression of the key. The period of the machine

/Was

Doc ID: 6587328

was 23 x 24 x 25 x 29 ~ 4 x 10^5. The following could give the daily key:- 1) Arrangement of the metal bars on the drum W. 2) Pin-setting of the three wheels A, B and C. 3) Cypher alphabet GA. The following was the setting for the message key:- 1) Initial position of drum W. 2) Initial position of the pin-wheels A, B and C. The following remarks may be made on the security of cypher-machine M 40:- As the machine was never used, we have no results of recent examination of its security to provide. Results obtained in 1939 were as follows:-

1) Owing to the restricted number of alphabets used, 10 messages on the same setting are sufficient to solve and reconstruct the machine.

2) A direct crib does not enable one to reconstruct the machine as, owing to the dummies, it is not possible to line up the clear text with the cypher text accurately enough.

3) An isolated cypher message cannot be broken.

4) Neither stereotype beginnings and endings, nor parallel pieces of text are compromising.

Thus, from results obtained at the time, it would appear that the machine had a relatively high degree of security. We do not know why it was not introduced. Cypher machine M 40 went through several stages of development before it took on its definitive form. Originally the drum remained stationary at every depression of the key, or gave one kick. Dummies were not intended at first. For a time the machine was fitted with an automatic morse transmitter. There was a key under each letter in the cypher alphabet. If this key were pressed, it caused the automatic transmission of this cypher letter by operating a sliding contact which brushed past morse-signals let in flush ((with the surface along which the sliding contact brushed)). We dropped this automatic transmission as it was too difficult to keep to five-letter groups.

Translator: M.G.F.

/Solution

Doc ID: 6587328

Solution of Japanese Diplomatic Messages

In the section dealing with JAPAN (Head of Section Oblt. Dr. ADLER), a few straightforward codes and simple recyphering systems were worked on and partly solved. Details of these operations are unknown to us.

Prof. Dr. FRANZ's cryptanalytic section worked on the following Japanese recyphering systems:

1) KOKOK messages: Messages with KOKOK, GAGAG etc., as indicator-groups produced numerous split-repeats, especially at the beginning of messages. As the relation between the number of vowels and the number of consonants was fairly exactly 50 : 50, it was suspected that a 2-letter vowel-consonant or consonant-vowel code was used. About 20 KOKOK messages were then written down one beneath the other, and the columns containing the minimum number of deviations, among adjacent bigrams, from the vowel-consonant or consonant-vowel form, were aligned together. This gave a transposition length of 19. This transposition was the same for all indicator-groups and remained so for months at a time.

2) So-called "Indicator-group messages" (J13).

Right at the start of our investigations, 2 messages on the PARIS-TOKIO link were discovered, of which the second was a repeat of the first, with slight differences. We were able to solve this pair of messages; the solution was facilitated by the fact that the basic code - the so-called LA code - was known. It was a 2-letter code recyphered by transposition; in the transposition cages, the first ten rows also contained blanks. The other messages with the same indicator supplied the basis of the actual code underlying these indicator-groups. With the knowledge of this basis, other indicator-groups could then be worked on successfully. On an average, 3 new indicator-groups appeared every day. The stencils remained in force for 10 days on an average. When the basic code happened to change, the new code was discovered by compromises that occurred.

After a year had gone by, the same indicator-groups recurred. Transposition systems and stencils were simply derived from those used in the previous year.

For the solution of these messages, the bigram apparatus was successfully introduced at Chi.

3) "KAIGUN" and "RIKUGUN".

Two attempts were made to solve the Japanese attache messages, but both were unsuccessful. As far as I can remember, nothing was discovered which might serve as a basis for a break-in.

4) Japanese machine

A few years ago, the German Foreign Office broke the Japanese machine messages, and constructed a machine of identical function to the Japanese one. When it was no longer

/possible

Doc ID: 6587328

to read the traffic, owing to alterations in the machine or to a different method of use, work on these messages was discontinued. In November, 1944, work was resumed by Baurat STEINBERG, but could not be concluded. It emerged, however, that the recypherment principle had remained the same.

5) Indicator-groups "FEVAZ" and "CIFOL"

All I can recall of the work on, and solution of, messages whose indicator-groups were generally "FEVAZ" or "CIFOL" is that the system consisted of recypherment, by substitution tables, of a basic code which also contained words in P/L. The contents of the messages were of a commercial nature.

Translator: J.M.E.

The Solution of Polish Attaché Messages

About 2½ years ago, when the cryptanalytic section took over work on Polish Attaché traffic, the subtractor used for recyphering was read off a figure-table horizontally and vertically. The table consisted of 24 lines, each containing 26 5-figure groups. In the margin of each table there were 100 different figure-bigrams from 00 to 99 in hatted order. Before each new line or column the appropriate margin-bigram from the table was inserted in the message text as an indicator. As the encypherers usually read off the subtractor horizontally and vertically in a serpentine fashion, the shape of the table could be reconstructed actually before the recovery of the book groups. In this way the whole of the encyphered material could be lined up together in depth and the recyphering groups "stripped" without any difficulty. We thus succeeded in reconstructing the code on a relative basis. The code showed a great number of groups of high frequency, and was thus particularly well suited for breaking the recypherment on a very small depth. After a series of tables had been reconstructed in this way this method of solution suddenly failed us. Neither did the known series of indicators appear any more. We presumed that the subtractor was now read off the table in another way. As we had got the book and many indicators occurred so frequently that were able to break messages recyphered on the same key, a study of the solved pieces of subtractor, for example, showed that the relative figure obtained for the 12th book-group after one indicator was identical with the relative figure obtained for the 7th book-group after another indicator. From this it was concluded that the supposed stencil had lain in such a position with both indicators that, in the first case, the 12th hole had lain in the position on the table where the 7th group lay in the second case. The indicator and the check-group indicated the co-ordinates of the top left-hand and bottom right-hand corners. If, with two different indicators, the stencil was moved only one digit to the right, then three digits of each relative figure for the second indicator were already obtained from the relative figure for the first indicator. Thus, by

/tedious

Doc ID: 6587328

tedious and close work, stencil, table and margin-bigrams were reconstructed. This work had to be carried out afresh for each new stencil, as the stencils were independent of each other. When the first stencil was solved, we were also able to restrict the relative basis of the basic code to 10 possibilities. We used Hollerith machines to help us. All the material belonging to one stencil and recyphering table was registered on Hollerith cards, i.e. against every message group its appropriate indicator and its position in the text were noted.

I can no longer remember details of the process of solution or characterisitics of the clear and cypher texts and cypher conventions. In any case it would never have been possible to find all three unknown quantities:- book, stencil and recyphering table - with the small amount of material on each key. With a knowledge of the code - and, at that, a code with very marked frequency peaks - there was latterly sufficient traffic to reconstruct table and stencil. If the windows had been made of various sizes in one stencil, it would not have been possible to solve the stencil - even with a known book.

By February, 1945, roughly 12 different stencils and a large number of tables had been solved. As far as we knew, the book remained the same all the time.

Translator: M.G.F.